National Infrastructure Advisory Council (NIAC)

Risk Management Approaches to Protection Working Group

Findings and Recommendations
October 11, 2005

Martha Marsh
President & CEO
Stanford Hospital and Clinics

Tim Noonan
Chairman, President & CEO
Internet Security Systems

Agenda

- NIAC Question
- Approach
- Findings
- Recommendations

NIAC Question

- "Can private sector experience with risk management and prioritization provide meaningful guidance to the President for risk management for national critical infrastructure planning and programs by the government?"
- NIAC cited private sector experience with risk management Experience includes managing IT and physical risk
  - Financial/commercial risk
  - Magnitude & duration of consequences
  - Customer & public impact by and acceptance of the consequences
  - Event experience, including:
    - Weather
    - Supply disruptions
    - Network disruptions
    - Commodity volatility
- NIAC identified methodological "gaps" for managing risks arising from:
  - Sector interdependencies
  - Catastrophic events
  - Cross-sector technology dependencies (e.g., SCADA)

Approach

Contributors to the study group included:

NIAC	Government	Academia	Industry
Finance	Homeland Security	Dartmouth	National Association of Corporate Directors
Technology	Defense	Maryland	North American Electric Reliability Council
Electric and Utilities	Municipal Government (Cobb County)	Stanford	Institute of Internal Auditors
Healthcare			Information Sharing and Analysis Council
Transportation			Partnership for Critical Infrastructure Security
Water			
Defense			
Communications			
Agriculture			
Others			

Approach (cont'd.)

- Assessed risk management methods and practices across industry, government and academia
- Academic risk management methodologies
  - Probabilistic Risk Analysis (PRA)
  - Stochastic Modeling
  - Bayesian Inference
- Private sector risk management standards
  - COSO
  - ISO
  - SOX
- Public sector risk management standards/studies
  - DHS RAMCAP
  - RAND "Urban Areas Risk" study
  - DoD (DCMA) Asset Prioritization Model
- Risk management studies
  - 1986 Challenger Accident
  - 9-11 Commission

Findings

- The group identified three high-level findings:
  - **FINDING #1:** Robust, standardized ***risk management methodologies***, supported by advanced technologies and infrastructure, maximize the effectiveness of risk management programs
  - **FINDING #2:** ***Risk management leadership***, a supporting organizational structure, and the development of a risk management culture enables the standardization of methods and enhances risk management program effectiveness
  - **FINDING #3:** Independent ***risk management oversight*** enhances strategic direction, focus, and accountability

Recommendations

- The Working Group made three high-level recommendations:
  - **RECOMMENDATION #1:** Create and standardize ***risk management methodologies*** and mechanisms for national planning and programs
  - **RECOMMENDATION #2:** Establish ***risk management leadership*** across the government for homeland security functions
  - **RECOMMENDATION #3:** Establish an independent ***risk management oversight*** function
- Details on recommendations follow

Recommendations (cont'd.)

- **RECOMMENDATION #1:** Create and standardize risk management methodologies and mechanisms for national planning and programs
  - Incorporate methodologies developed and employed successfully in the private sector into national risk management system; adopt "best of breed" for each industry; implement forward-looking risk management models
  - Continue to develop mechanisms to identify, acquire, and collect risk management data
  - Continue to develop improved/advanced risk management methodologies

Recommendations (cont'd.)

- **RECOMMENDATION #1 (cont'd):** Create and standardize risk management methodologies and mechanisms for national planning and programs
  - Standardize and disseminate risk management methods across the government (similar to HSPD-7 framework); Develop and implement framework (outlined in Recommendations #2 and #3) to facilitate distribution and use of standardized methodologies
  - Seek and retain expert opinions in the field of risk management
  - Ensure that actionable information is disseminated to all stakeholders

Recommendations (cont'd.)

- **RECOMMENDATION #2:** Establish risk management leadership across government for homeland security functions
  - At Risk Management Program Level:
    - DHS should continue to serve as government-wide risk management program lead (e.g. comparable to the corporate Office of the Chief Risk Officer) for Homeland Security matters
    - Define and disseminate standardized risk management methodologies
    - Coordinate government-wide Risk Council; Function as government-wide Risk Acceptance Authority
    - Analyze and prioritize threats to the critical infrastructures and establish priorities
  - At Sector-Specific Agency Level:
    - Serve as single, senior focal point for sector specific risk management (similar to corporate business unit Director of Risk Management role); define organizational assumptions; function as the organizational Risk Acceptance Authority
    - Employ standardized risk management methods and infrastructure (tailored for the sector) as part of the risk mitigation strategy
    - Make risk management recommendations to organizational lead
    - Assume responsibility for risk assessment and management coordination with owner and operator stakeholders

Recommendations (cont'd.)

- **RECOMMENDATION #3**: Establish independent risk management oversight function
  - At Risk Management Program Level:
    - Establish a body responsible for risk management oversight (functions similar to corporate Board of Directors); establish, at the senior-most level, a risk management culture
    - At a strategic level, establish risk management metrics, including incentives and penalties
    - Validate risk assessment and management methodologies
    - Validate decisions (assumptions) of the Risk Acceptance Authorities; validate priorities
  - At Sector-Specific Agency Level:
    - Provide sector specific risk management oversight; ensure compliance with strategic risk management program (functions similar to Board Audit Committee)
    - Validate decisions (assumptions) of the organizational Risk Acceptance Authority; validate priorities
    - At an operational level, establish risk management metrics, including incentives and penalties